1. Поєднання технічних та організаційних заходів для захисту ОІД;

Захист інформації з обмеженим доступом при автономному використанні на ОІД пристроїв обробки інформації здійснюється шляхом створення комплексу ТЗІ, який складається із сукупності:

-     організаційних заходів захисту від несанкціонованих дій з інформацією (для захисту конфіденційної інформації, що є власністю держави або вимога щодо захисту якої встановлена законом);

-     організаційних заходів захисту від несанкціонованих дій з інформацією та технічних засобів захисту інформації від витоку технічними каналами за наявності можливості створення таких каналів (для захисту інформації, що становить державну таємницю).

У залежності від умов розташування об’єктів встановлені категорії норм за визначеними для кожного виду технічних засобів (ТЗ) каналах витоку інформації:

1 категорія – встановлюється для об’єктів інформаційної діяльності (ОІД) де циркулює інформація що складає відомості з грифом (ОВ);

2 категорія – встановлюється для об’єктів інформаційної діяльності (ОІД) де циркулює інформація що складає відомості з грифом (ЦТ);

3 категорія – встановлюється для об’єктів інформаційної діяльності (ОІД) де циркулює інформація що складає «таємні» відомості.

2. Засоби захисту телефонних ліній зв’язку.

Пасивні засоби захисту мають за мету ослабити рівень небезпечного сигналу у АТЛ. Дія пасивних засобів захисту АТЛ передбачає: – блокування небезпечних сигналів від елементів телефонного апарата внаслідок так званого “мікрофонного ефекту”; – фільтрацію небезпечних сигналів від пристроїв високочастотного нав’язування; – від’єднанння джерел (перетворювачів) небезпечних сигналів, наприклад, акустичних закладок, що передають інформацію телефонною лінією в режимі покладеної трубки.

Для блокування низькорівневих сигналів від “мікрофонного ефекту” використовуються нелінійні розв’язувальні пристрої,

Дія активних засобів полягає у накладанні захисного шуму на небезпечний сигнал. Розрізняють низькочастотні маскувальні сигнали в діапазоні від 100 Гц до 10 кГц та високочастотні широкосмугові – від 20 кГц до 30 МГц. Внаслідок ефекту маскування не вдається засобами технічної розвідки виділити інформативні параметри сигналів витоку. Активні засоби блокування технічних каналів витоку абонентськими телефонними лініями часто називають засобами лінійного зашумлення, а їхня дія ґрунтується на створенні і «закачуванні» в лінію при покладеній трубці шумового сигналу. Генератори шуму ГШ під’єднуються в розрив телефонної лінії і монтуються, як правило, безпосередньо в корпусі телефонного апарата (рис. 6). Шумовий сигнал подається в лінію в режимі, коли телефонний апарат не використовується (трубка покладена). При піднятті трубки телефонного апарата подавання в лінію шумового сигналу припиняється.

Якщо інформаційна атака по телефонному каналу здійснюється за рахунок підключення до лінії зв’язку радіозакладного пристрою контактного типу з живленням від самої лінії, тоді такі пристрої змінюють характеристики самої лінії, що може бути зафіксованим приладами або системами аналізу стану телефонної лінії. Отримання такої інформації може бути приводом для висновку про несанкціонований доступ до даної лінії. Наприклад, підключення радіозакладок або телефонних ретрансляторів такого типу призводить до зміни значення живлячої напруги телефонної станції. Для виміру напруги та струму витоків в лінії може використовуватись, наприклад, прилад ТСМ-03.

Фільтрація небезпечних сигналів використовується для захисту телефонних апаратів від “ВЧ нав’язування”. Як правило, для захисту телефонних апаратів використовують пристрої, котрі об’єднують фільтр та обмежувач. Це пристрої типу “Экран”, “Гранит-8” і “Гранит-10”, “Корунд”, “Грань-300” та ін.

Відключення апарату від лінії при проведенні конфіденційних переговорів є найбільш радикальним методом захисту. Для автоматичного відключення при покладанні слухавки використовують виріб типу “Барьер-М1” .

До сертифікованих засобів лінійного зашумлення відносяться пристрої МП-1А (захист аналогових телефонних апаратів) та МП-1ЦП-1А (захист числових телефонних апаратів) та ін.

Низка активних методів захисту телефонних ліній складає функціональні можливості сукупних можливостей трьох пристроїв захисту, таких як “Прокруст”, “Протон”, “Цикада-М”. Окрім зазначених пристроїв широко використовують пристрої моделей “Sel SP-17/P”, “Гром-3И-6”, “Кзот-06” та інші. Ефективність пристроїв активного захисту телефонних ліній оцінюють за їх спроможністю протистояти тим чи іншим методам інформаційної атаки.

Для передавання цифрової інформації використовують пристрої серії СМ: кишеньковий телекс-шифратор СМ-11, шифратор для телефаксів СМ-13, радіоперемовний чотириканальний пристрій СМ-21 для діапазону 134….174 мГц, та ін.